Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт Космических и Информационных Технологий
институт
Вычислительная техника
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ О. В. Непомнящий
подпись инициалы, фамилия
«___» _____ 20 __ г.

БАКАЛАВРСКАЯ РАБОТА

09.03.01 «Информатика и вычислительная техника»
код и наименование специальности

Моделирование работы сети на основе стандарта IEEE 802.11
и оценка ее устойчивости средствами OMNet++
тема

Руководитель	_____ подпись, дата	доцент, канд.техн.наук. должность, ученая степень	О. А. Русанова инициалы, фамилия
Выпускник	_____ подпись, дата		А. Д. Пронин инициалы, фамилия
Нормоконтролер	_____ подпись, дата		В. И. Иванов инициалы, фамилия

Красноярск 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Беспроводные компьютерные сети – это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей (например, Ethernet), без использования кабельной проводки. Такие сети используются как корпоративные сети внутри зданий, для связи удаленных отделений между собой, а так же в общественных местах, такие как парки, рестораны и площади.

Разработкой стандартов аппаратного обеспечения вычислительных сетей занимается институт инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers, IEEE). Эта общественная некоммерческая ассоциация специалистов появилась в 1963 году, главной целью которой является информационная и материальная поддержка развития научной деятельности в электротехнике, электронике, компьютерной технике и информатике.

Основной группой стандартов семейства IEEE являются стандарты 802. Службы и протоколы, указанные в IEEE 802 находятся на двух нижних уровнях модели OSI: физический и канальный. Стандарт 802.11 является рабочей группой занимающейся беспроводной локальной сетью и базовым стандартом для всех последующих версий спецификаций 802.11a/b/g/n.

Можно выделить следующие достоинства данной технологии:

- Беспроводные технологии не требуют использования кабеля внутри сети, что значительно понижает стоимость оборудования;
- Точки доступа беспроводной сети способны обеспечить высокие скорости передачи до 600 Мбит/с, что значительно превышает скорость проводной передачи Ethernet 10Мбит/с или Fast Ethernet 100 Мбит/с;
- Беспроводной доступ в интернет можно обеспечить в местах, где нет возможности или не выгодно прокладывать кабель. Технология Wi-Fi является гибкой в построении и позволяет быстро организовать временные сети;

- Мобильность клиентов дает возможность перемещения в пределах зоны покрытия, что отбрасывает потребность проводов и фиксированного рабочего места;
- Так же стоит отметить высокую совместимость различных типов сетевых устройств, например, ноутбуки и телефоны, и оборудования с поддержкой стандартов беспроводных сетей.

1 Анализ предметной области

1.1 Топологии беспроводных сетей

На начальном этапе планирования беспроводной сети необходимо учесть типы оборудования с поддержкой различных стандартов, технологии настройки точек доступа, это может быть индивидуальная настройка или централизованная, а так же методы построения сети, то есть типы соединения, способы передачи и доступа к внешней сети.

Дальше будут рассмотрены основные технологии, позволяющие расширить зону покрытия беспроводной сети, путем объединения нескольких точек доступа в единую сеть без необходимости наличия проводного соединения между ними.

1.1.1 WDS

Благодаря системе беспроводной рассылки (Wireless Distribution System, WDS) точки доступа могут объединяться в единую сеть с любыми Wi-Fi устройствами, расширяя при этом зону покрытия. Точка доступа WDS может работать в режиме Wi-Fi-моста и в режиме репитера или повторителя.

Основные базовые станции, как правило, подключены к проводной сети и в зависимости от выбранного режима являются источником беспроводной сети, тогда как релейные станции или повторители служат для связи основных удаленных устройств, выполняя функцию усилителя и ретрансляции сигнала.

Как сказано ранее WDS может обеспечивать два режима для соединения точек доступа:

- Первый режим беспроводного моста предоставляет защищенный доступ между устройствами от других клиентских устройств, которые сообщаются между собой;

- Второй режим выполняет функцию повторителя.

Обязательным критерием для настройки станции WDS является использование одной и той же частоты, метода и ключа шифрования. Настройка имени точки доступа или SSID может быть разной.

Перечислим преимущества использования технологии WDS:

- Простота настройки и подключения;
- Отсутствие проводного соединения между точками доступа Wi-Fi;
- Использование одного канала позволяет быстро перестроить топологию в случае ошибок;
- Сохранение MAC-адресов клиентов сети.

Не смотря на простоту реализации технологии, разделяют следующие недостатки:

- Пропускная способность сети сокращается на 50%, по сравнению с проводным подключением;
- Отсутствие гарантии совместимости между разными производителями;
- Так как номер канала должен быть всегда постоянным, существует гарантия появления другой станции с тем же каналом, что приведет к наложению сигналов и понижению пропускной способности;
- Устаревшее оборудование поддерживает шифрование только WEP.

1.1.2 Mesh

Технология Mesh это децентрализованная, одноранговая организация ячеистой топологии между узлами сети. Узлы в данной сети предоставляют собой услуги абонентского доступа и выполняют функции маршрутизаторов для других узлов, входящих в эту же сеть. Вследствие чего появляются масштабируемые зоны покрытия сети с активными узлами.

Подобные технологии используются в военных целях для объединения ведомостей разных стран в зонах военных конфликтов, для создания опера-

тивной связи в стратегических целях. Получили распространенное применение в телекоммуникационных сетях для передачи данных. В Mesh-сетях есть возможность объединения локальных сетей (Local Area Network, LAN) и городских сетей (Metropolitan Area Network, MAN) с возможностью интеграции в глобальные сети (Wide Area Network, WAN), что является отличительной чертой технологии.

Сети в Mesh делятся на территории покрытия, так же называемы кластерные зоны, количество которых не ограничено. В каждом кластере располагается от восьми до шестнадцати узлов. Одна точка доступа имеет выход во внешнюю сеть интернет, а остальные узлы соединяются между собой по общему радиоканалу, выполняя функции повторителей.

В протоколах, описывающих функции Mesh-сетей, каждый абонент сети создает собственную оптимальную динамическую таблицу маршрутизации до каждого устройства. При отказе одного из устройства, происходит определение нового маршрута и обновление таблицы.

Основное применение Mesh используется для объединения удаленных регионов в одну общую независимую от провайдеров сеть со своей уникальной топологией. Стоит отметить, что протоколы Mesh используют шифрование всего трафика, что повышает безопасность сети. Так же используется авто-конфигурируемая маршрутизация с возможностью объединения через внешнюю сеть.

1.1.3 Ad Hoc

Технология Ad Hoc так же относится к децентрализованному типу беспроводной сети. Сеть называется Ad Hoc, потому что она не относится к сетям с ранее существующей инфраструктурной, что является одноранговым соединением. Например, роутеры в проводных сетях, которые контролируют трафик в проводных сетях или точки доступа в управляемой беспроводной сети. Вместо этого каждый узел участвует в маршрутизации посредством пе-

ренаправления данных на другие узлы, то есть детерминирование данных происходит динамически на каждом соединении, с помощью существующих алгоритмов маршрутизации.

Рассмотрим преимущества беспроводной Ad Hoc сети:

- Высокая производительность сети;
- Дешевизна оборудования;
- Использование лицензированных полос пропускания;
- Быстрая рассылка трафика источника.

К недостаткам относятся следующие пункты:

- Динамическая топология за счет мобильности клиентов;
- Необходимость высокой степени адаптивности сетей;
- Отсутствие центрального оборудования;
- Требует дополнительные более сложные методы маршрутизации.

Сети Ad Hoc так же разделяют по принципу маршрутизации. Всего существует три категории протоколов маршрутизации:

1) Проактивный или табличный принцип (англ. proactive, table-driven). С данной настройкой точки доступа периодически рассылают по сети фреймы или служебные сообщения, содержащие информацию обо всех изменениях в ее топологии. На основе данной информации каждый узел сети строит собственную таблицу маршрутизации до всех остальных узлов, откуда маршрут считываются при необходимости передачи сообщения какому-либо адресу назначения.

2) Реактивный принцип или работающий по запросу (англ. reactive, on-demand). При данном способе каждая точка доступа составляет таблицу маршрутизации до конкретных узлов только при возникновении необходимости в передачи информации. Для этого узел-отправитель рассылает широковещательный запрос-сообщение по всей сети, которое должно дойти до узла-адресата. В ответ адрес назначения высылает сообщение о подтверждении, в котором указывается необходимый маршрут, после чего информация

записывается в таблицу маршрутизации. Для повторной отправки сообщения данному адресату маршрут считывается из таблицы. Если обнаруживается разрушение связи с узлом назначения, то запускается процедура поддержания маршрута, которая заключается в поиске нового маршрута до адресата.

3) Гибридные (англ. hybrid). Данный принцип комбинирует механизмы проактивных и реактивных методов. Сеть разбивают на множество подсетей, внутри которых работает проактивный протокол, а взаимодействие между подсетями осуществляется реактивными методами. В крупных сетях это сокращает размеры таблиц маршрутизации для каждого узла, теперь им необходимо знать только маршруты до узлов подсети, к которой они принадлежат. Также сокращается объем служебной информации, рассылаемой по сети, так как основная часть распространяется лишь в пределах подсетей.

По времени построения маршрута проактивные протоколы обладают явным преимуществом перед реактивными, так как проактивным протоколам необходимо лишь считать маршрут из таблицы. В то время как реактивные протоколы работают по требованию, рассылая широковещательный запрос, что занимает соответствующее время для отправки запроса до адреса назначения и времени ожидания ответа. Однако проактивным так же необходимо постоянно распространять широковещательные рассылки для обновления таблиц, что занимает значительную долю пропускной способности.

Вывод: В связи с вышеизложенными способами построения сети, мною выбрана технология Ad Hoc. Сети Mesh строятся для территориального объединения между регионами, что несет сложную организацию сети и сильную мобильность топологии. Технология WDS не подходит из-за простоты реализации, низкой надежности и отсутствием динамических протоколов. В сетях Ad Hoc существуют реактивные протоколы создающие маршруты по требованию и не загружают трафик частыми обновлениями в таблицах, что удовлетворяет заданной сети с частым появлением новых клиентов.

1.2 Протоколы беспроводной сети

Разработкой стандартов для сетей занимается отдел 802 организации IEEE (Institute of Electrical and Electronic Engineers). В 1997 году комитетом 802.11 принят стандарт для беспроводной сети, который определял функции MAC-адресов канального уровня модели OSI и определяет набор протоколов для самых низких скоростей передачи данных (transfer).

Из всех существующих стандартов на практике наиболее часто используются всего четыре, это: 802.11a, 802.11b, 802.11g и 802.11n.

1.2.1 Физические уровни протоколов 802.11a/b/g

Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11, предусматривая скорость передачи данных до 54 Мбит/с. В отличии от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a обеспечивает повышение скорости передачи за счет использования полосы частот шириной 300 МГц из диапазона частот 5 ГГц. Так как полоса частот в этом диапазоне шире, то в зависимости от правил регулирования конкретной страны их может быть 48 и более. К недостаткам стандарта 802.11a относится более высокая потребляемая мощность радиопередатчиков и меньший радиус действия.

В спецификации 802.11b института IEEE по-прежнему используется диапазон 2,4 ГГц. Для повышения скорости до 11 Мбит/с здесь применяется более эффективный вариант метода DSSS, опирающийся на технику Complementary Code Keying (CCK), заменившую код Баркера. Диапазон 2,4 ГГц с шириной полосы примерно в 80 МГц разбит на 14 каналов, каждый из которых, кроме последнего, отстоит от соседей на 5 МГц.

Для передачи данных согласно стандарту 802.11b используется полоса частот шириной в 22 МГц, поэтому появляется необходимость объединения несколько соседних каналов для того чтобы гарантировать некоторый мини-

мум взаимных помех, возникающих от передатчиков. Например, использование трех каналов 1, 6 и 11 для трех сетей, с учетом того, что они не накладываются друг на друга, как видно на рисунке 1.

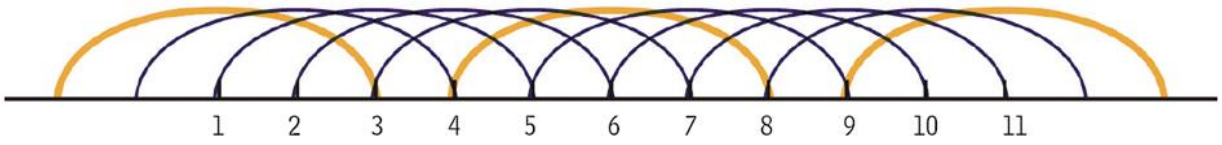

Рисунок 1 – Разбитие диапазона 2,4 ГГц на каналы

Этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей, из-за предусмотренного в этом стандарте автоматического понижения скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11g разработан рабочей группой института IEEE в 2003 году. Является логическим развитием 802.11a, который обеспечивал те же скорости до 54 Мбит/с и развитием стандарта 802.11b, работающий в том же диапазоне 2,4 ГГц. Основной причиной роста популярности новой спецификации стало то, что стоимость оборудования стандарта 802.11g достаточно быстро приравнялась со стоимостью оборудования стандарта 802.11b.

1.2.2 Физический уровень протокола 802.11n

Стандарт 802.11n принят в октябре 2009 года. Включает в себя множество усовершенствований по сравнению с устройствами стандарта 802.11g. Так, например, они могут работать в одном из двух диапазонов как 2.4 ГГц, так и в диапазоне 5 ГГц. Рекомендуемый диапазон является диапазон 5 ГГц благодаря большему числу доступных каналов и меньшей интерференции с многочисленным оборудованием, работающих в диапазоне 2,4 ГГц.

На физическом уровне реализована усовершенствованная обработка сигнала и модуляции. На канальном подуровне управления реализовано более эффективное использование доступной пропускной способности. Вместе эти усовершенствования позволяют увеличить максимальную теоретическую скорость передачи данных до 600 Мбит/с, что значительно больше, по сравнению с 54 Мбит/с стандарта 802.11a/g.

Вместо каналов с полосой в 20 МГц, которые использовались в технологиях 802.11a и 802.11g, в технологии 802.11n применены каналы с полосой 40 МГц, так же допускается использование каналов в 20МГц. Расширение полосы в два раза должно приводить к повышению битовой скорости, а так же при усовершенствованном кодировании частотного мультиплексирования с разделением каналов (OFDM), вместо 52 первичных несущих частот на полосу в 20 МГц здесь используется 56 таких частот, а на полосу в 40 МГц соответственно 114. Это приводит к повышению битовой скорости с 54 до 65 Мбит/с для каналов 20 МГц и до 135 Мбит/с для каналов 40 МГц.

Для надежного распознавания кодовых символов в технологиях 802.11a/g используется межсимвольный интервал в 800 нс. Технология 802.11n позволяет передавать данные с таким же межсимвольным интервалом, а так же с межсимвольным интервалом в 400 нс, что повышает битовую скорость для каналов 40 МГц до 150 Мбит/с.

Применение техники MIMO (Multiple Input Multiple Output - множественные входы и выходы) позволяет использовать несколько антенн сетевого адаптера с целью лучшего распознавания сигнала, пришедшего к приемнику разными путями. Из-за таких эффектов распространения радиоволн, как отражение, дифракция и рассеивание, приемник получает несколько сигналов, дошедших от передатчика по разным физическим путям и имеющим сдвиг по фазе. До появления техники MIMO во избежание таких негативных последствий, в каждый момент времени использовалась только одна антенна, которая принимала сигнал лучшего качества.

В системе MIMO существует одно преимущество, которое называется пространственным мультиплексированием. Благодаря этому появилась возможность обрабатывать несколько независимых потоков данных, переданных с помощью нескольких антенн. Типичной системой MIMO стандарта 802.11n является система 3 × 3 : 2, то есть система с тремя передающими и тремя принимающими антеннами, которая позволяет передавать два независимых потока данных. Это обеспечивает повышение битовой скорости в два раза, то есть до 300 Мбит/с для каналов 40 МГц. Стандарт 802.11n предусматривает различные варианты системы MIMO вплоть до 4 × 4 : 4, что повышает битовую скорость до 600 Мбит/с.

1.2.3 Технология Ad Hoc сетей протокола 802.11s

Стандарт IEEE 802.11s это улучшенный стандарт для протоколов IEEE 802.11, определяющий тип взаимодействия беспроводных устройств, которые используется для создания фиксированной топологии в сетях Ad Hoc и Mesh.

Стандарт 802.11s работает на втором уровне, уровне MAC-адресов модели OSI, и определяет архитектуру, поддерживающую как широковещательные (broadcast), так и мультикастовые (multicast) способы доставки. Так же определен юникастовый (unicast) способ доставки, использующий метрику радиовещания поверх самонастраивающийся топологии с большим количеством промежуточных узлов.

Для выбора оптимальных маршрутов в сети используются метрики. Метрики включают в себя такую информацию, как длина пути, пропускная способность, стоимость передачи трафика, загрузка, надежность, задержка.

Наиболее распространенной метрикой является длина пути, то есть количество переходов, через которые проходят данные от источника к получателю. Длина пути, в данном случае, это количество переходов от источника до адреса назначения по узлам сети.

Метрика, связанная с пропускной способностью, отражает степень занятости сетевых ресурсов, таких как каналы и маршрутизаторы. Загрузка вычисляется различными способами, например, загрузки процессора и числом обрабатываемых или передаваемых в секунду пакетов. Следует отметить, что постоянный анализ этих показателей требует значительную занятость ресурсов сетевого оборудования.

Так же используется надежность. Под «надежностью» подразумевается доля потерь пакетов в каждом из каналов, которые имеют свойства разрыва или потери связи, на что уходит время для восстановления связи и поиска нового оптимального маршрута.

Другая часто использующаяся метрика – задержка, которая рассчитывает необходимое время для доставки пакета от источника к получателю. Задержка зависит от таких факторов, как пропускная способность канала, очереди в портах узлов на пути пакета, загрузка сети всех промежуточных каналах, а так же физическое расстояние, которое нужно преодолеть.

Метрика стоимости существенно отличается от перечисленных выше критериев. Некоторые компании предпочитают использовать пути через собственные платные каналы других операторов, а не через более высокопроизводительные.

Так же метрика отдельных каналов может быть статической и динамической. Статическая метрика задается администратором сети и а такой метрикой может быть, например, стоимость. Существенно отличается динамическая метрика, которая может изменяться по задержке пакетов, уровню сигнала и множеству других параметров. Причем она может определяться без дополнительных служебных пакетов и использовать специальные «пробные» запросы для сбора статистики каждого канала.

Стандарт IEEE 802.11s вводит обязательный критерий для совместимости устройств, чтобы все устройства поддерживали метрику времени передачи в канале. В основе метода выбора пути для передачи данных в стандарте 802.11s лежит механизм профилей. Этот механизм обеспечивает совмести-

мость устройств от разных производителей, которые могут поддерживать как стандартизованные механизмы, так и собственные. В профиль входят следующие данные: идентификатор профиля, идентификатор протокола маршрутизации, идентификатор метрики протокола маршрутизации. Устройство может поддерживать несколько профилей работы, но единовременно лишь один из них может быть активным.

Вывод к главе: в связи расширением ширины пропускания и методов передачи трафика развитие стандартов беспроводной сети привело к более надежному соединению и передачи данных на высоких скоростях, сравнимых только с проводной сетью. На сегодняшний день основными протоколами беспроводной сети являются стандарты 802.11b/g/n. Так же с уверенностью можно сказать, что данные версии стандарта встроены во все современные устройства с поддержкой беспроводного соединения. Поэтому данные три версии стандарта выбраны как основные. Так же рассмотрен расширенный протокол 802.11s, который используют в сетях Ad Hoc и Mesh.

1.3 Безопасность беспроводной сети

С появлением беспроводной локальной сети, главной задачей стало повышение качества безопасности передачи как коммерческих, так и не коммерческих данных. Как и любая компьютерная сеть, сеть Wi-Fi часто подвергается несанкционированным атакам. Кроме того, проникнуть в беспроводную сеть значительно проще, чем в проводную. Достаточно оказаться в зоне приема сигнала.

Основная безопасность беспроводных сетей обеспечивается на физическом и канальном уровнях модели OSI. Для защиты применяются математические модели аутентификации, шифрование данных и контроль целостности их передачи, тем не менее, вероятность взлома данных является весьма существенной.

1.3.1 WAP

Одним из ранних алгоритмов обеспечения безопасности беспроводных сетей, разработанных в 1997 году, является спецификация WEP (Wired Equivalent Privacy). В WEP применяется общий ключ, который может использоваться в качестве аутентификации или шифрования пакетов данных. Данный ключ известен только при взаимном обмене меду двумя устройствами, это узел сети и точка доступа.

В WEP применяется алгоритм шифрования RC4, состоящий из 40 разрядов 64-разрядного ключа и 24-разрядного вектора инициализации. Для повышения безопасности беспроводных сетей, данный алгоритм был расширен до 128-разрядного и более длинного ключа, состоящий из 104-разрядной и более длинной пользовательской части и вектора инициализации. Поэтому, разделяют две разновидности WEP, это WEP-40 и WEP-104.

В настоящее время данный метод защиты информации является устаревшим и не рекомендован к использованию, так как выявлены его уязвимости и слабые места, например, способ аутентификации и алгоритм шифрования.

1.3.2 WPA/WPA2

На замену технологии защиты беспроводной сети WPA пришла спецификация WAP. Версии WPA и WPA2 (Wi-Fi Protected Access) является обновленной программой сертификации устройств беспроводной связи и обеспечивает более высокую защиту от нежелательного взлома информации. Так же отличительной характеристикой является множественная совместимость между беспроводными устройствами как на аппаратном, так и на программном уровнях. На данный момент разработкой WPA занимается организация Wi-Fi Alliance.

В новом методе защиты информации WPA присутствует поддержка шифрования в соответствии со стандартом AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования), который имеет ряд преимуществ над технологией WEP RC4. Приведем некоторые особенности WPA:

- Усовершенствованная схема шифрования;
- Аутентификация с использованием протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации);
- Централизованная система безопасности.

Основная проблема WEP заключается в использовании слишком похожих ключей для пакетов данных. Эту задачу решает новый протокол целостности временного ключа TKIP (Temporal Key Integrity Protocol). Протокол TKIP отвечает за увеличение размера ключа с 40 до 128 бит с автоматическими генерирующимися ключами. В данной методике используется специальная иерархия ключей и управления ими, которая уменьшает излишнюю предсказуемость, использованной в WEP. Применяется динамическая генерация ключей шифрования с использованием двустороннего ключа, которая используются для шифрования каждого пакета данных. Подобная иерархия заменяет статический ключ WEP на 500 миллиардов возможных ключей, используемых для шифрования.

Так же стоит обратить внимание на основные режимы шифрования WPA-Personal и WPA-Enterprise, отличающиеся как способом аутентификации, так и методом использования.

Для большинства домашних сетей используется режим WPA-Personal или WPA-PSK (Pre Shared Key). В данном варианте после установки пароля на точку доступа, пароль распространяется на всех пользователей и он должен вводиться вручную при аутентификации каждым пользователем индивидуально.

Этот режим является не безопасным, так как данный пароль хранится на беспроводных устройствах. И любой авторизированный пользователь с доступом к сети, может подключиться к устройству, а также увидеть пароль. Поэтому рекомендуется использовать данный режим в домашней сети.

Второй режим называется WPA-Enterprise или RADIUS. Данный режим сложнее в настройке и является централизованным управлением доступа с индивидуальной пользовательской аутентификацией. То есть при подключении к сети, каждый пользователь должен иметь личную учетную запись для авторизации.

Этот режим предполагает установку RADIUS-сервера, который работает по протоколу 802.1x. При такой настройке, пользователь не имеет дела с ключами шифрования. Каждый ключ назначается во время каждой пользовательской сессии в фоновом режиме после предоставления личных данных серверу. Данный режим шифрования обычно используется в корпоративных офисах или учебных заведениях.

Вывод: Методы шифрования являются важной часть беспроводных сетей, обеспечивающие защиту информации от нежелательного проникновения. На сегодняшний день WPA2 является самым распространенным методом шифрования, имея два режима доступа, это WPA-Personal с заранее известным паролем и WPA-Enterprise с установкой RADIUS-сервера и индивидуальными настройками для каждого пользователя.

1.4 Анализ зоны покрытия

Проанализируем особенности распространения электромагнитных волн. Чем выше частота, тем хуже проникает сигнал через препятствия. Низкочастотные радиоволны, например, АМ-диапазоны, легко проникают в дома, а более высокочастотный сигнал телевидения требует внешней антенны.

Сигналы в диапазоне выше 30 МГц распространяются только по прямой, то есть являются сигналами прямой видимости. При частоте свыше 4 ГГц сигнал начинает поглощаться водой, то есть простой туман может стать причиной ухудшения качества передачи волны.

Так же стоит учитывать проблемы поведения сигналов, распространяющихся в режиме прямой видимости и встречающих на своем пути препятствия. Встретившись с препятствием, сигнал может распространяться в соответствии с тремя механизмами: отражением, дифракцией и рассеиванием.

При учете факторов влияющих на поведение сигнала необходимо проанализировать зону покрытия лесного участка, пролегающего между Лыжной базой СФУ и Госуниверситетом на Свободном проспекте. На протяжении всего маршрута проложена брусчатка шириной примерно 1,5 метра. На всем пути расставлены фонарные столбы на расстоянии друг от друга в 15-30 метров, на которые впоследствии планируется установка точек доступа.

Особое внимание стоит уделить типу местности. Выбранный участок представляет собой площадь с растущими вокруг густыми деревьями, со значительным постепенным перепадом высот, примерно в 50-75 метров, как видно из рисунка 2.

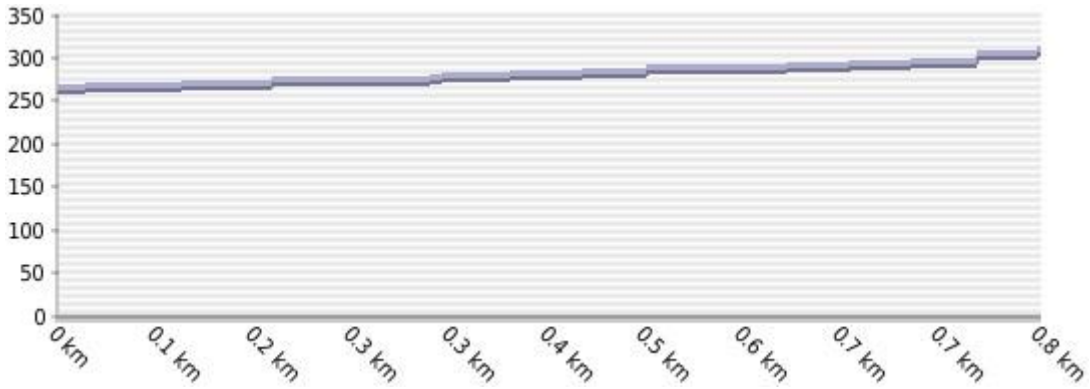

Рисунок 2 – График перепада высот

При использовании беспроводной точки, поддерживающих стандарт 802.11n, с коэффициентом усиления антенны 3 дБи, зона покрытия Wi-Fi равняется примерно 150-300 метров в условиях местности без преград. В помещении эта цифра равняется 50 метрам. Такие препятствия, как кирпичные стены, металлические элементы и деревья могут значительно уменьшить радиус действия. Даже листва деревьев может стать препятствием, так как содержит воду, которая поглощает микроволновое излучение данного диапазона. Например, проливной дождь ослабляет сигнал до 0,05 дБ/км, густой туман на 0,02 дБ/км, а деревья, ветви и листва до 0,5 дБ/метр. В итоге радиус действия беспроводной точки в условиях выбранной местности будет варьироваться между 50-75 метров.

Проанализирован густой лесной участок за библиотекой СФУ. Маршрут показан на рисунке 3. Общая протяженность данного участка составляет примерно 970 метров.

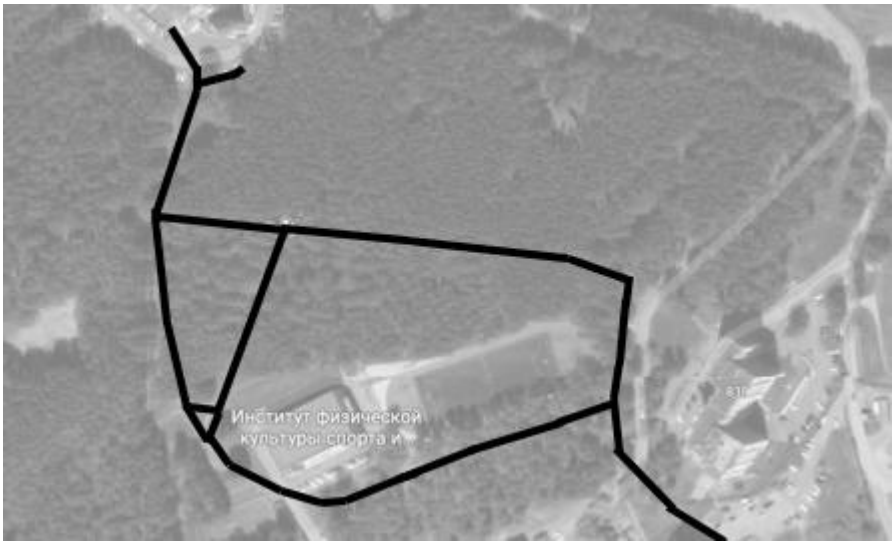

Рисунок 3 – Маршрут за библиотекой СФУ

Сложность данного участка заключается в отсутствии прямой видимости между фонарными столбами, за счет большого количества деревьев, что является значительным препятствием распространению волн. Данная мест-

ность не будет смоделирована из-за сложности топологии и большого количества факторов влияющих на распространение сигнала.

Так же точно проанализирован лесной участок области Березовой Рощи. Выявлено, что на протяжении всего проложенного маршрута по обе стороны асфальта области обставлены незначительным количеством деревьев. И все же найдены места, где между фонарными столбами в прямой видимости в виде препятствия стоят деревья. Хоть несущая волна имеет свойство дифракции, такие зоны будут проанализированы при постройке топологии в программном обеспечении OMNet++ для выявления решений данной задачи.

Карта, выше описанного лесного участка, протяженностью примерно в 830 метров, показана на рисунке 4. На протяжении всего маршрута расставлено 32 фонарных столба. Первые 340 метров столбы расположены по левую сторону, остальной промежуток в 490 метров столбы стоят справа. Такое же количество точек доступа, сколько и фонарных столбов, потребуется для построения избыточной топологии.

Рисунок 4 – Лесной участок Березовая Роща

Сделаем вывод. При анализе лесного участка выявлено, что основным фактором, влияющим на распространение сигнала, являются деревья, так как дерево и листва содержат воду, а вода поглощает огромную часть сигнала. Участок за библиотекой СФУ не был выбран из-за сложности топологии и большого количества деревьев, что является затруднительным для анализа поведения сети. Основным участком выбрана Березовая Роща, по причине небольшого количества деревьев и малого перепада высот. Так же для установки точек беспроводного доступа выбраны фонарные столбы, которые расставлены на протяжении всего маршрута.

1.5 Обзор программного обеспечения OMNet++

OMNet++ - это объектно-ориентированная модульная система сетевого моделирования. У него есть архитектура наследования, поэтому он используется в различных областях, таких как:

- Моделирование проводных и беспроводных сетей
- Моделирование протоколов
- Моделирование сетей массового обслуживания
- Моделирование мультипроцессоров и других аппаратных систем
- Оценка показаний сложных программных систем

OMNet++, как таковой, не является симулятором, а скорее представляет собой инфраструктуру для написания симуляций. Одной из фундаментальной части этой инфраструктуры является компонентная архитектура для имитационных моделей. Модели собраны из многократно используемых компонентов, называемых модулями. Хорошо написанные модули можно использовать многократно, а так же комбинировать их между собой различными способами.

Модули соединяются друг с другом через ворота или порты, и объединяться для формирования составных модулей. Глубина вложенных модулей не ограничена. Они обмениваются сообщениями, которые могут нести произвольные структуры данных. Модули передают сообщения по заранее определенным путям через ворота или непосредственно к месту назначения, что очень полезно для беспроводной симуляции. Модули на самом низком уровне иерархии называются простыми модулями, инкапсулируя поведение модели. Простые модули программируются на языке C++ и используют библиотеку симуляций.

Система OMNet++ поддерживает параллельное распределенное моделирование. Например, MPI (Massage Passing Interface, Интерфейс передачи сообщениями), разработанный Уильямом Гроуппом, Эвином Ласком и другими. Это программный интерфейс для передачи информации, который позволяет обмениваться сообщениями между процессами, выполняющими одну задачу.

По вышеперечисленным пунктам, можно сделать вывод, что модульная система сетевого моделирования OMNet++ может использоваться в качестве моделирования протоколов беспроводной сети и проектирования зоны с покрытием доступа Wi-Fi, так как имеет поддержку программирования стандартов и оценку показаний систем.

Вывод: В данной главе рассмотрены основные технологии построения топологии и взаимодействия беспроводного оборудования. Выбрана основная технология построения маршрутизации на основе сети Mesh с использованием стандарта 802.11s. Проанализированы протоколы взаимодействия точек доступа с конечными устройствами, поддерживающих стандарты беспроводной сети, и выбраны основные, это 802.11b/g/n, которые широко распространены на сегодняшний день, и, использующиеся всеми типами мобильных устройств и ноутбуков. Выбраны необходимые устройства и составлены их структурные схемы. Так же приведен обзор на среду моделиро-

вания OMNet++, в которой будет собрана и проанализирована работа составленной сети.

2 Проектирование

2.1 Структурная схема

На начальной стадии построения беспроводной Mesh сети разработана схема, показанная на рисунке 5. Данная схема определяет основные функциональные части сети, их назначение, взаимосвязи между ними и отображает принцип действия сети в самом общем виде.

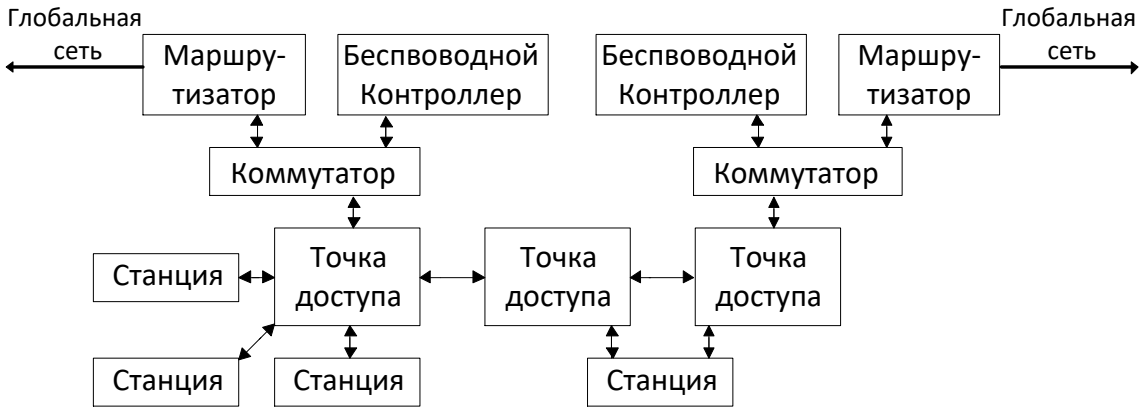

Рисунок 5 – Структурная схема беспроводной Ad Hoc сети

Структурная схема содержит следующие функциональные части:

- Маршрутизатор обеспечивает непосредственно саму маршрутизацию, то есть взаимодействие между основной сетью Ad Hoc и доступом в глобальную сеть.
- Контроллер беспроводной сети, является отдельным устройством, обеспечивающий конфигурацию точек доступа.
- Коммутатор является промежуточным устройством между маршрутизатором, контроллером беспроводной сети и первой точной доступа. Выполняет задачи коммутации между соединениями.

- Точка доступа является устройством, раздающим интернет-трафик по беспроводному соединению хостам. Так же, данное устройство, позволяет создавать Ad Hoc сеть.
- Станция является конечным устройством, которое может быть представлена в виде мобильного устройства или ноутбука.

2.2 Функциональная схема

На рисунке 6 показана функциональная схема, предназначенная для разъяснения процессов в отдельных частях сети.

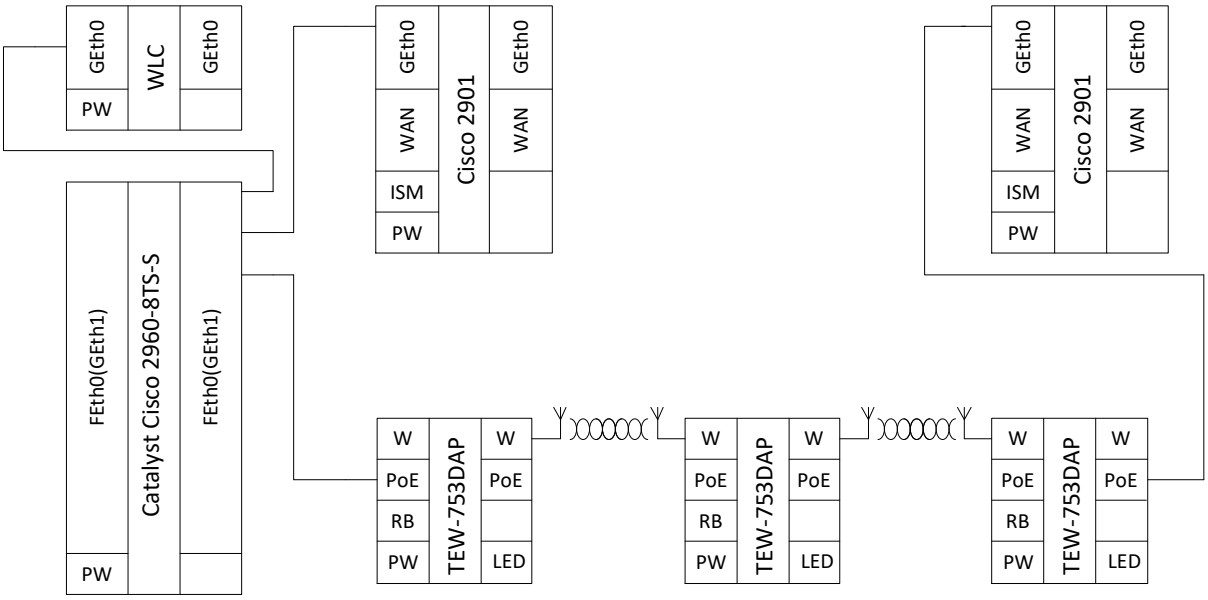

Рисунок 6 – Функциональная схема беспроводной Ad Hoc сети

На рисунке 6 показана общая функциональная схема беспроводной сети. В качестве точки доступа выбрано устройство типа TEW-753DAP. Эта двухдиапазонная точка доступа работает на втором и третьем уровнях модели OSI с MAC и IP-адресами. Так же она поддерживает такие беспроводные стандарты, как 802.11a/b/g/n с допустимой скоростью от 11 Мбит/с до 300 Мбит/с. На функциональной схеме видно, что точки доступа передают друг

другу информацию посредством беспроводного соединения. Данное соединение обеспечивается с помощью технологии Ad Hoc.

Поддержка двух диапазонов 2,4 ГГц с коэффициентом усиления сигнала в 3 дБи и частотой 5 ГГц с коэффициентом усиления сигнала в 4 дБи дает в логарифмическом пересчете усиление сигнала в 2 и 2,5 раза соответственно. Стоит учитывать и выходную мощность сигнала в 17 дБм стандарта 802.11n, что позволяет повысить скорость до 300 Мбит/с. Исходя из этих данных можно примерно определить зону покрытия беспроводной сети на открытой плоскости без препятствий в 150-300 метров.

С учетом вышеизложенного можно сказать, что данная точка доступа удовлетворяет нашим условиям, а именно позволяет нам создать Ad Hoc сеть используя диапазон 5 ГГц, и сеть для беспроводного доступа к сети для клиентов.

Коммутатор выбран версии Catalyst Cisco 2960-8TS-S. Этот коммутатор работает на втором уровне модели OSI с MAC-адресами, обеспечивая стандартную коммутацию между устройствами.

Так же данный коммутатор содержит восемь портов Fast Ethernet с пропускной способностью 100 Мбит/с и одним портом Gigabit Ethernet с пропускной способностью 1 Гбит/с. Так как наша сеть не требует создания усложненных коммутационных топологий, данный коммутатор, с небольшим количеством портов, удовлетворяет нашим требованиям, обеспечивая взаимодействие между точками доступа, маршрутизатором и контроллером.

В качестве маршрутизатора выбрана модель Cisco 2960. Этот маршрутизатор работает на третьем уровне модели OSI с IP-адресами и имеет два порта Gigabit Ethernet с пропускной способностью 1 Гбит/с и двумя портами WAN, обеспечивающие доступ во внешнюю сеть, скорость которых задается типом кабеля, либо сами провайдером сети интернет.

Так же выбран контроллера беспроводной сети типа Cisco WLC. Основная задача беспроводного контроллера состоит в динамической конфигурации точек доступа и хостов, разделяющий доступ на виртуальные сети, с

помощью протокола DHCP и метода доступа VLAN. Данное устройство является стандартным для использования удаленной настройки точек доступа и присвоения уникального IP-адреса новым узлам, поэтому оно полностью удовлетворяет нашим требованиям.

Вывод: В этой главе разработана структурная схема, определяющая основные функциональные части работы сети и функциональная схема, наглядно разъясняющая процессы взаимодействия устройств внутри сети. Подобраны типы оборудования, разобраны технические характеристики каждого устройства, их особенности и необходимость использования.

3 Реализация спроектированной схемы сети в OMNet++

3.1 Описание использованных модулей

В процессе реализации спроектированной схемы сети в OMNet++ использованы встроенные модули протоколов, устройств и алгоритмы взаимодействия между ними. Далее описаны некоторые из них.

Для импорта модуля, необходимо воспользоваться командой import. Использован модуль сценарий ScenarioManager, в котором необходимо указать определенные команды, которые будут выполняться в указанное время. Команды сценария записывается в файл формата xml, где команды могут нести одно из следующих действий:

- Изменение значения параметра;
- Изменение какого-либо атрибута подключения, например, задание частоты ошибок в битах;
- Удаление или добавление соединения или передача команды указанному модулю;

Данный модуль позволяет полностью управлять заданной сетью, удалять или добавлять маршруты в таблицу маршрутизации, принудительная отправка трафика через указанный протокол. При использовании перечисленных операций, необходимо учитывать, что заданный протокол поддерживает эту команду.

Настройка сценариев включает в себя следующие шаги:

1. Добавление экземпляра ScenarioManager в сетевую модель;
2. Создание фала с форматом xml и установка параметров сценария;

Дополнительно к модулю сценария необходимо добавить модуль LifecycleController, который управляет такими операциями, как закрытие, перезагрузка, приостановление, возобновление работы для отдельных узлов

(маршрутизаторы, точки доступа, хосты и так далее) и является исполнительным модулем написанного сценария.

При разработке учтена физическая среда, которая оказывает глубокое влияние на взаимодействие беспроводных устройств. Например, физические объекты, такие как стены зданий, деревья и листва. В главе анализа зоны покрытия описана анализируемая местность и основными объектами, влияющими на распространение сигнала, являются деревья.

С учетом окружения, необходима визуализация физических объектов. За это отвечает встроенный класс PhysicalEnvironment, который отвечает за управление препятствий. Препятствия так же указываются в отдельно созданном файле формата xml, где объекты определяются его формой, расположением, ориентацией, материалом и способом отображения. Формат xml позволяет использовать предопределенные форы как куб, призма, многогранник и сфера, при этом есть возможность задания собственного материала.

Стоит отметить модуль под названием radioMedium. Все беспроводные симуляции в INET нуждаются модуле радиосвязи. Этот модуль представляет собой разделяющий физический передатчик, который отвечает за распространение сигнала, затухание, помех и других физических явлений. На физическом уровне существуют различные реализации модуля радиосвязи. Например, IdealRadioMedium, который является самой простой моделью и такие явления, как ослабление сигнала, игнорируются, а диапазон связи указывается в метрах.

Для представления более реалистичной среды необходимо использовать схемы модуляции с использованием APSKScalarRadio, что использует различные методы передачи сигнала, такие как амплитудная фазовая манипуляция (Amplitude Phase Shift Keying, APSK), квадратурная фазовая манипуляция (Quadrature Phase Shift Keying, QPSK) и квадратурная амплитудная модуляция (Quadrature Amplitude Modulation, QAM). Это необходимо для моделирования затухания и поведения сигнала при столкновении с препятствием. Дополнительная особенность модуля APSKScalarRadio состоит в ими-

тации преамбулы и заголовка на физическом уровне во время передачи пакетов, длины которых может быть установлена вручную.

В качестве визуализации использовался подмодуль visualizer модуля IntegrateCanvasVisualizer, который способен отображать пути пакетов используя параметр routeVisualizer. Этот модуль отображает путь между узлами, по которому прошел отправленный пакет. Путь отображается как цветная стрелка, проходящая через промежуточные хосты. Отображение постоянно исчезает и появляется через определенное количество времени. Данный модуль позволяет проследить правильность перемещения пакета и маршрут, который выбрал использованный протокол.

Так же использовалась статическая маршрутизация. Статическая настройка в INET Framework выполняется с помощью конфигурационных модулей IPv4, включая назначение адресов и добавление маршрутов, которая выполняется с помощью модуля IPv4NetworkConfigurator. Для этого также используется спецификация xml формата.

При обращении к конфигуратору о назначении IP-адреса в диапазоне 10.0.0.x, модуль создает маршруты на основе оценочной частоты ошибок пакетов между узлами. То есть в этот момент конфигуратор рассматривает беспроводную модель в виде графа, где узлы с высоким коэффициентом ошибок будут иметь высокую стоимость, а с низким коэффициентом ошибок будут иметь низкую стоимость.

3.2 Построение беспроводной топологии

Для оценки устойчивости топологии беспроводной сети, средствами OMNet++ смоделирована сеть, содержащая пять беспроводных точек доступа, расположенные примерно на расстоянии пятидесяти метров друг от друга и конечное устройство, поддерживающее беспроводное соединения в виде мобильного устройства. Расстояние определяется расположением устройств

на стенде графической части программы в файле DStend.ned. Листинг программы приведен в Приложении А. Описанная модель показана на рисунке 7.

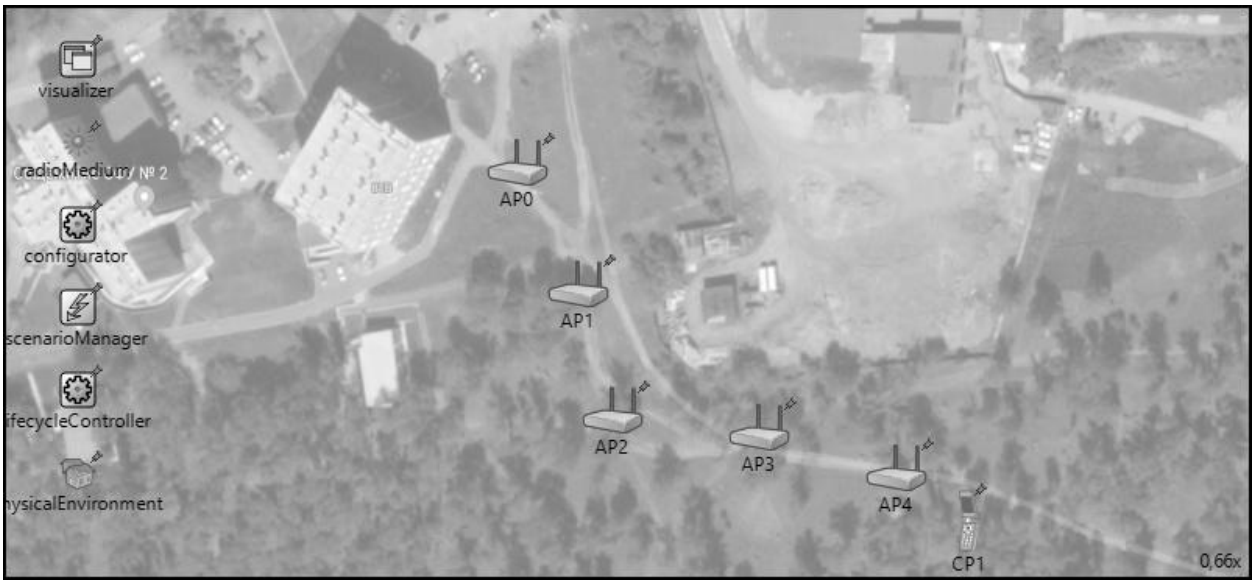

Рисунок 7 – Смоделированная беспроводная сеть

Произведен ряд экспериментов с использованием различных методов маршрутизации и контроля надежности передачи трафика. Реализация разных конфигураций позволит детально проанализировать способы построения топологии беспроводной сети и сделать выводы на полученных результатах.

Первый эксперимент разделен на два этапа: имитация трафика без подтверждения доставки и с подтверждением доставки. Для этого настроена статическая маршрутизация, с использованием модуля конфигурации IP-адресов для каждого устройства. Это необходимо, что бы каждая точка доступа имела личный IP-адрес и знала маршрут до удаленного устройства, не входящего в ее зону покрытия.

Так же включена интерференция на каждом устройстве с удвоенным значением радиуса действия точек доступа. Радиус покрытия настроен таким образом, что каждое устройство видело только своих соседей. Интерференция позволяет сымитировать поведение трафика при наложении сигналов

друг на друга, при появлении такой ситуации пакеты отбрасываются, и переданная информации искажается.

В качестве постоянного трафика использовался протокол пользовательских дейтаграмм (User Datagram Protocol, UDP). Источником трафика UDP выбрано мобильное устройство, а устройством назначения точка доступа AP0, с частотой отправки пакетов равной экспоненте числа двенадцать, что дает увеличение трафика с каждой отправкой и позволяет отследить поведение сети на большой поток пакетов данных.

На первом этапе при передаче трафика не настроена операция подтверждения получения пакета на каждом устройстве. В результате в течение минуты отправлено 5041 пакетов, а принято всего 2203 пакетов. Больше пятидесяти процентов потери пакетов, объясняется наложением сигналов друг на друга, что приводит к интерференции и неправильной обработке полученных данных. Наглядное представление интерференции показано на рисунке 8.

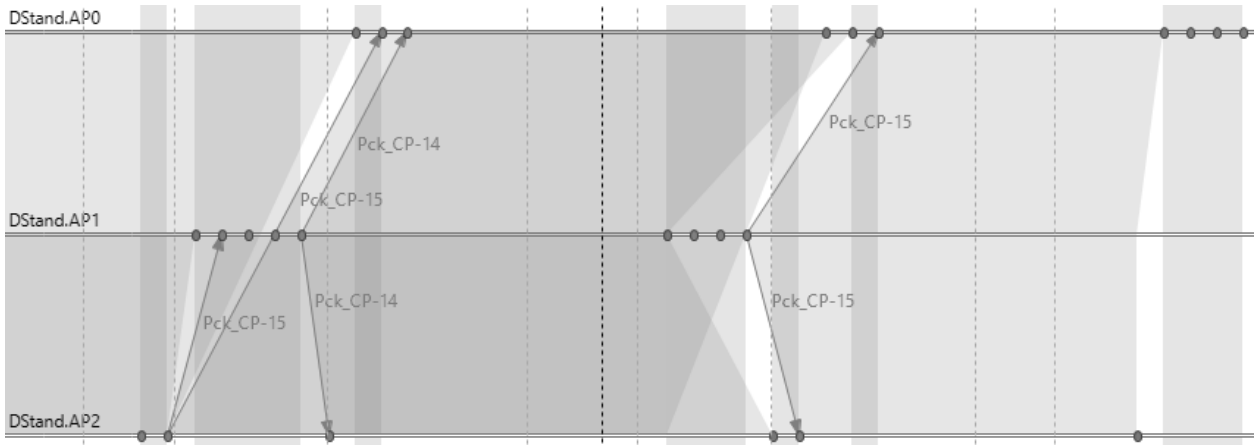

Рисунок 8 – Интерференция сигналов

В момент передачи пятнадцатого пакета под названием Pck_CP-15 точкой доступа AP2, сигнал принимает точка AP1. При этом сигнал так же доходит до точки AP0, но он не может быть обработан, так как до него доходит лишь остаточный сигнал, с большим количеством шумов. Дочка AP1 широ-

ковещательно отправляет принятый ранее четырнадцатый пакет, который доходит до точки AP0 и AP2, во время передачи пятнадцатого пакета. Наложение сигналов приводит к искажению данных, в результате чего оба пакета отбрасываются.

Второй этап заключается в добавлении технологии множественного доступа с прослушиванием несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection, CSMA/CD). Данный метод говорит сам за себя. Если при намерении передачи пакета одним из устройств, станция обнаруживает другой сигнал, занимающий среду, она устанавливает таймер (transmitionTimer) и после ожидания времени задержки снова предпринимает отправить кадр. Так же после получения пакета одним из устройств, оно отправляет подтверждение (CsmaAck). В результате добавления технологии CSMA/CD в течение минуты отправлено 4983 пакета и принято 4983, что означает при передаче не потеряно ни одного пакета. Процесс передачи кадров показан на рисунке 9.

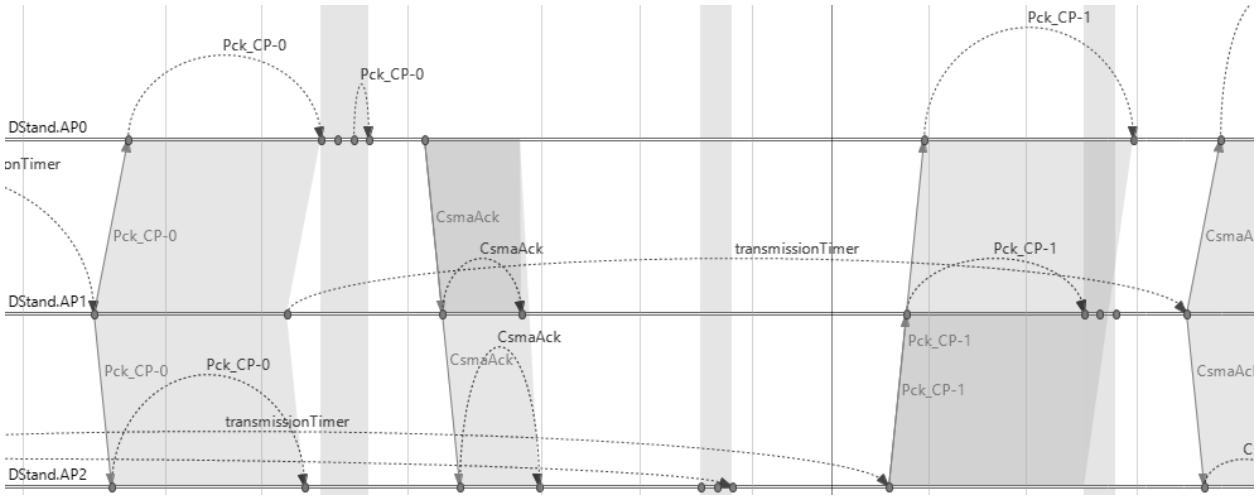

Рисунок 9 – Использование множественного доступа

Данный эксперимент показывает необходимость прослушивания частоты и подтверждение полученных данных, так как моделированием доказа-

но, что при интерференции несущие накладываются друг на друга и обработка сигнала становится невозможной.

Выше описанные методы построены на статической маршрутизации, то есть при появлении клиента в зоне видимости сети, пользователь не будет добавлен в таблицу маршрутизации, как конечный узел, и он не будет иметь доступа во внешнюю сеть. Поэтому во второй эксперимент добавлен протокол динамической маршрутизации и добавлен модуль мобильности устройств, для имитации передвижения клиента.

В программном обеспечении OMNet++ реализован реактивный протокол динамической маршрутизации для мобильных Ad Hoc-сетей (Ad Hoc On-Demand Distance Vector, AODV). Поэтому в качестве построения мобильной сети заданной топологии используется данный модуль.

Протокол AODV является реактивным, то есть составляет маршруты до указанных узлов только при необходимости. Использует служебные сообщения, которые наследуют концепцию hello-пакетов, рассылаемые устройством своим соседям в переделах видимости, для поддержания списка их активности, что позволяет ускорить процесс построения маршрута.

Когда один из конечных хостов пытается отправить кадр, точка доступа отправляет широковещательный запрос на составление маршрута (Route Request, RREQ) всем видимым узлам. Другие точки сети AODV также пересылают этот пакет в общую среду и делают запись об источнике запроса. Когда устройство, знающее об адресе назначения, получает пакет RREQ, он посылает сообщение с ответом (Route Reply, RREP) через тот же маршрут отправителю. В таком случае узел назначения выбирает наименьший маршрут до адреса источника и через некоторое время простоя запись маршрута удаляется из таблицы маршрутизации. Стоит отметить, что в сетях AODV существует возможность настройки сообщения подтверждения (RREP Acknowledge Number, RREP-ACK).

В результате процесса моделирования AODV сети в течение минуты отправлено 4961 UDP-пакетов, получено 4468. Примерный процент потери

кадров составляет 10%. Это можно объяснить тем, что часть времени потрачено на первичное определение маршрута и на последующее подтверждения каждого полученного пакета.

После клиенту CP1 добавлена мобильность, передвижение производится по линейной плоскости относительно четвертой, третей и второй точек со скоростью 2 м/с. В результате мобильным устройством отправлено 4961 пакетов, а доставлено до назначения 4458. Во время передвижения клиент обнаружил три точки доступа, каждый раз запускалась процедура обнаружения маршрута, что заняло некоторое время. Процедура обнаружения маршрута показана на рисунке 10, где видно описанный ранее метод построения маршрута по требованию. Время поиска маршрута от начала запроса клиента до начала отправки кадра, согласно моделированию, составляет 816.8 мс.

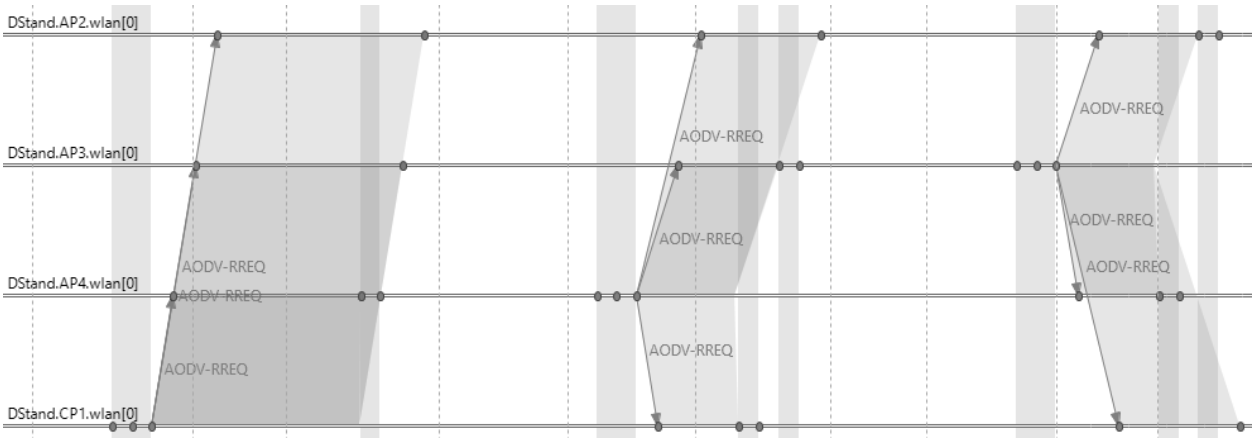

Рисунок 10 – Процедура обнаружения маршрута

В третий эксперимент добавлен сценарий отключения одной из точек доступа на определенный период, для вычисления времени восстановления сети. Написанный сценарий, отключает на семь секунд устройство AP2, которое является промежуточным узлом сети. Для того чтобы сеть продолжала работать, диапазон действия увеличен до таких размеров, чтобы каждая точка доступа входила в радиус сети как минимум двух последующих узлов, это создает избыточную топологию.

В результате отключения точки доступа AP2, пакет не прошел по найденному маршруту и ближайший к нему узел широковещательно разослал сообщение об ошибке (Route Error, RERR). Процесс оповещения об ошибке показан на рисунке 11. Сообщение дошло до узла отправителя и операция вычисления нового маршрута запустилась заново с сообщения RREQ. Перестройка сети с момента отключения устройства AP2 до момента определения другого маршрута и отправки нового пакета, по результатам моделирования, примерно прошло время равное 1 секунд и 238.5 мс, что примерно в полтора раза превышает нахождение маршрута на начальном этапе. Это обусловлено тем, что выявление неисправности оборудования занимает примерно 110 мс и исправление таблицы маршрутизации каждого узла сети AODV, так же требует время.

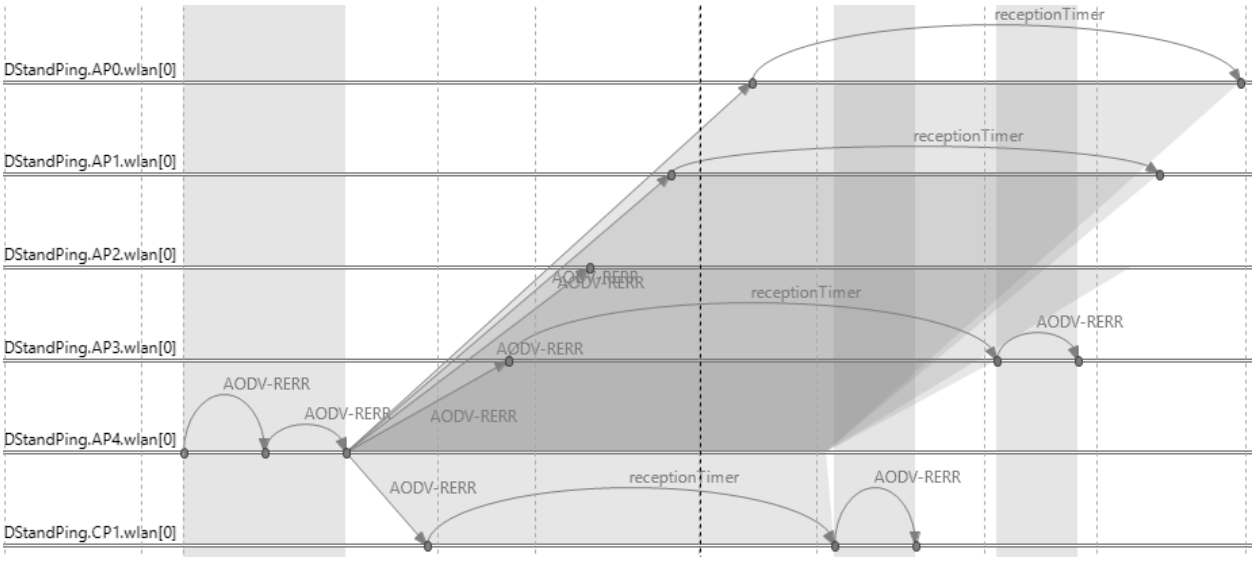

Рисунок 11 – Кадр об ошибки маршрута

Так же необходимо смоделировать пересечение сигнала с объектом, в данном случае это дерево, и добавить более чувствительную настройку каждому устройству. Это будет заключительная часть четвертого эксперимента.

Для написания окружения используется соответствующий модуль. Объекты расставлены между точкой доступа AP2 и AP3, как и следовало

ожидать, во время моделирования, сигнал полностью поглотился деревьями, и передачи пакета не осуществилась.

Чтобы решить задачу рассеивания, использован модуль представления более реалистичной среды, описанный в предыдущей главе. В данном модуле не используется радиус действия точки в метрах, вместо этого устанавливается порог чувствительности опорной мощности в единицах измерения децибел на мВт. Данное значение выбрано в соответствии с протоколом 802.11n равной -76 дБм. Основная несущая частота установлена в 2.4 ГГц и ширина пропускания 20 МГц.

Мощность передатчика для беспроводных точек доступа составляет 75-100 мВ, а для мобильных устройств 50 мВ. Данные значения являются большими для моделирования сети, поэтому они уменьшены до 10 мВ и 3.5 мВ для каждого типа устройства соответственно. Так же существует параметры настройки длины передачи преамбулы и размера заголовка пакета, которые установлены в 10 мкс. и 10 бит. Настроен коэффициент усиления антенны в 3 дБ.

Данные настройки позволяют проанализировать поведение сигналов на границах чувствительности и приблизить моделирование к более реалистичным условиям. В результате моделирования сети с написанными объектами в виде деревьев, результат показал, что препятствия не ограничили передачу сигнала и благодаря описанной конфигурации сеть работает более стабильно.

Составлена диаграмма, показывающая краткую сводку общего количества полученных и отправленных пакетов данных за различные типы конфигурации сети, показана на рисунке 12.

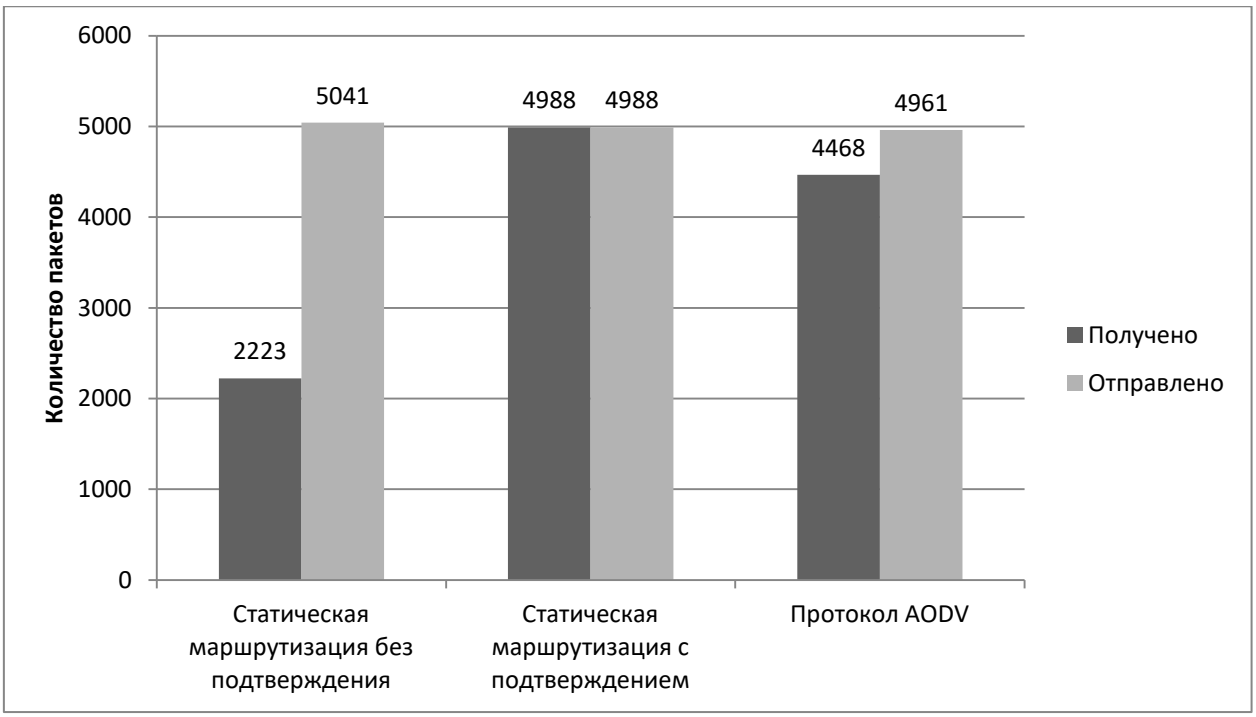

Рисунок 12 – Диаграмма сравнения надежности доставки
с разными параметрами конфигурации

В качестве расширения четвертого эксперимента добавлено несколько пользователей для повышения нагрузки трафика и проверки надежности доставки. Данные стенд показан на рисунке 12. Добавлено два конечных устройства CP2 и CP4 расположенных рядом с точкой доступа AP0, отправляющие запрос ping до узла AP4. Для каждого добавленного устройства так же будет производиться собственное вычисление маршрута до адреса назначения, начиная с обмена запросов AODV-RREQ между промежуточными узлами и заканчивая пакетами AODV-RREP, подтверждающие составление маршрута.

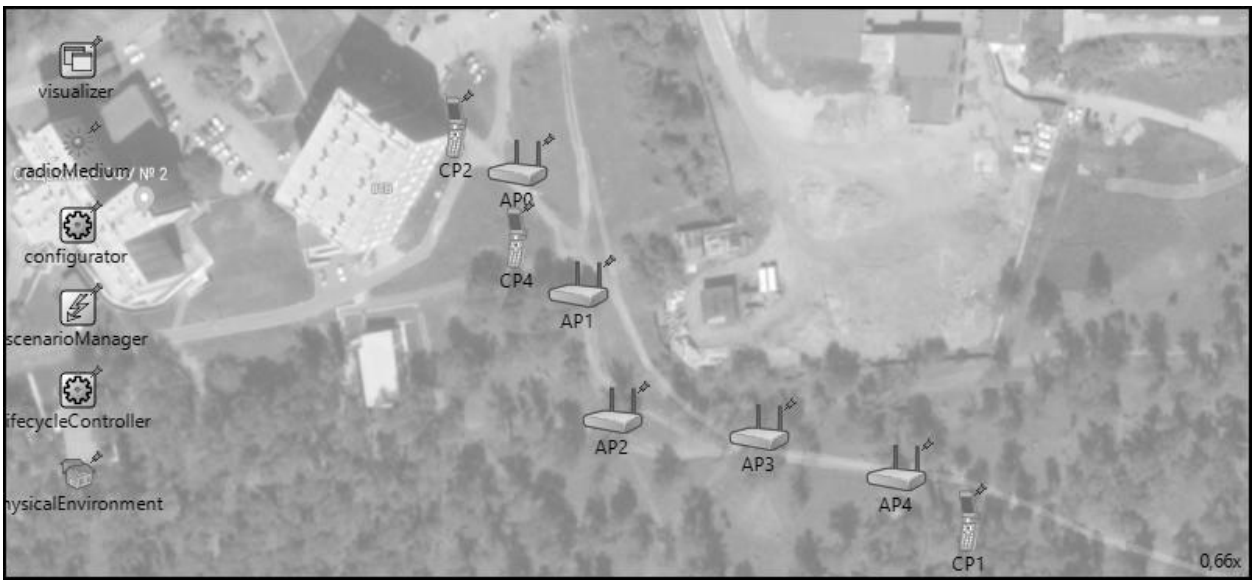

Рисунок 13 – Расширенный стенд с добавленными мобильными устройствами

В результате моделирования описанной сети мобильным устройством CP2 отправлено 4984 UDP пакетов и получено 4678. Так же устройствами CP2 и CP4, с экспоненциальным интервалом 50 мс и 70 мс соответственно, производилась дополнительная нагрузка отправкой трафика запросами ping до узла AP0. Хостом CP2 отправлено 1219 кадров и получено 1124, а хостом CP4 отправлено 826 кадров и получено 825. Результаты эксперимента показаны на рисунке 14.

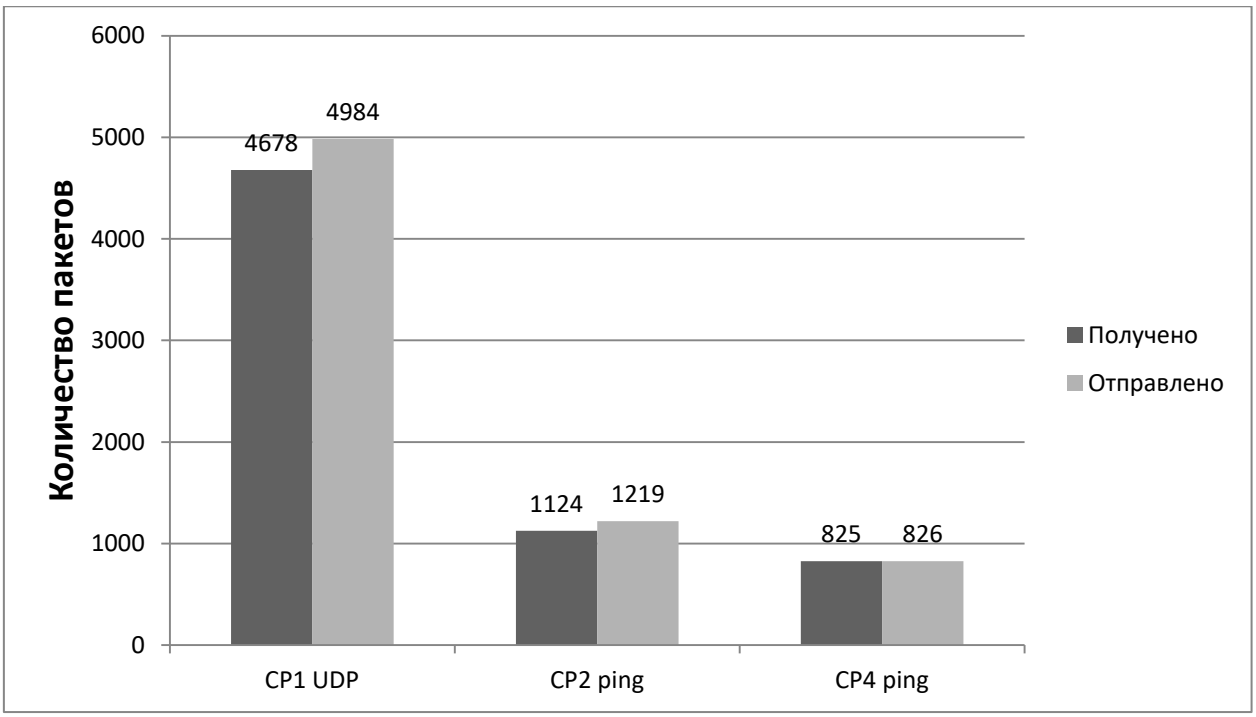

Рисунок 14 – Диаграмма сводки полученных и отправленных пакетов с дополнительной нагрузкой трафика

Вывод: В результате различных экспериментов моделирования сети средствами OMNet++, выявлены основные проблемы при построении беспроводной сети связанные с нахождением маршрутов в мобильной топологии и проанализированы трудности надежности доставки в условиях различной нагрузки трафика. Детально описана процедура нахождения маршрута с использованием динамического протокола AODV. Проанализирован механизм и время перестройки сети при отказе одного из устройств. Использован модуль чувствительной настройки узлов, для приближения моделирования к более реалистичным условиям.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы, посвященной моделированию работы сети на основе стандарта IEEE 802.11 и оценки ее устойчивости средствами OMNet++, проанализированы технологии и особенности работы беспроводной сети.

Рассмотрены методы построения топологии беспроводной сети, основанные на технологиях WDS, Ad-Hoc и Mesh, в результате чего выбрана технология Ad Hoc. Приведены методы безопасности беспроводной сети, такие как WAP, WPA и WPA2 и разобраны отличия основных режимов работы WPA-PSK и WPA-Enterprise. Так же описаны стандарты взаимодействия беспроводной точки доступа и конечных узлов. Такими стандартами являются сертификаты IEEE 802.11g и 802.11n.

На начальном этапе моделирования сети разработана структурная схема для общего понимания работы беспроводной связи и проанализирована предоставленная зона покрытия лесного участка. В результате чего сделаны выводы об особенностях местности, описаны причины, которые могут повлиять на распространение сигнала. Фонарные столбы выбраны как места для установки оборудования, расстояние между которыми удовлетворяют зоне покрытия беспроводных точек и позволяют создать избыточную топологию на случай отказа одного из устройств. Найдены участки для дальнейшего моделирования и анализа поведения сети.

Основной программой для моделирования сети выбрано программное обеспечение OMNet++. Данная программа подходит для написания протоколов разных уровней, для моделирования проводных и беспроводных сетей и позволяет проанализировать работу сети с помощью графов, собирая полученную информацию в ходе симуляции сети.

Разработана функциональная схема для разъяснения процессов, происходящих в отдельных функциональных частях сети в целом. В ходе построе-

ния функциональной схемы подобраны типы оборудования, описаны характеристики и принципы работы каждого устройства.

Средствами OMNet++ смоделирована беспроводная сеть с использованием уже существующей реализации протоколов и устройств, встроенных в программное обеспечение OMNet++. Произведен анализ работы составленной топологии и приведена статистика построения сети AODV и перестройки топологии в связи потери связи с одним из устройств. Результаты приведены и проанализированы в виде графиков, построенных после сбора данных смоделированной сети.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Базовые-положения-стандарта-IEEE-802-11n-для-сетей-Wi-Fi [Электронный ресурс] : Режим доступа: https://help.keenetic.net/hc/ru/articles/213968809

2. Безопасность в сетях WiFi. WEP, WPA, WPA2 шифрование Wi-Fi [Электронный ресурс] : Компания «Гет Вайфай» предоставляет весь спектр услуг, связанных с построением беспроводных сетей связи. 2006-2014. – Режим доступа: http://www.getwifi.ru/psecurity.html

3. Беспроводные компьютерные сети [Электронный ресурс] : Режим доступа: https://dicom.spb.ru/articles/network-and-servers/wireless-computer-networks/

4. Выходная мощность сигнала передатчика [Электронный ресурс] : Цифровая техника в радиосвязи. 2001-2017. – Режим доступа: http://digteh.ru/UGFSvSPS/power/

5. ГОСТ 2.701–2008 Единая система конструкторской документации. Схема. Виды и типы. Общие требования к выполнению. дата введ. 01.07.2009. – Москва: Стандартинфором, 2009. – 17с.

6. ГОСТ 2.702-2017 Единая система конструкторской документации. Правила выполнения электрических схем. дата введ. 01.01.2012. – Москва: Стандартинформ, 2011. – 28 с.

7. ГОСТ 2.710–81 Единая система конструкторской документации. Обозначения буквенно-цифровые в электрических схемах. Взамен ГОСТ 2.710–75; дата введ. 01.07.1990. – Москва: Издательство стандартов, 1985. – 17 с.

8. ГОСТ 2.743–91 Единая система конструкторской документации. Обозначения условные графические в схемах. Элементы цифровой техники. дата введ. 01.01.1993. – Москва: Издательство стандартов, 2000. – 45 с.

9. ГОСТ 7.80–2000 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Заголовок. Общие требова-

ния и правила составления. дата введ. 01.07.2001. – Минск: Издательство стандартов. 2000. – 11 с.

10. ГОСТ 7.82–2001 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления. дата введ. 01.07.2002. – Минск: Издательство стандартов. 2001. – 26 с.

11. ГОСТ 21.406–88 Система проектной документации для строительства. Проводные средства связи. Обозначения условные графические на схемах и планах. дата введ. 01.07.1989. – Москва: Стандартинформ, 2010. – 46 с.

12. Двухдиапазонная точка доступа Wi-Fi N 600 Мбит/с [Электронный ресурс] : Официальный сайт TRENDnet в России. 2018. – Режим доступа: https://www.trendnet.com/langru/products/wifi/N-access-points/N600/TEW-753DAP#tabs-solution02

13. Коммутаторы [Электронный ресурс] : Сайт Кунегина Сергея Владимировича. 2000-2014. – Режим доступа: http://kunegin.com/ref1/net_dev/switch.htm

14. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание. Стандарт третьего поколения. / В. Олифер, Н. Олифер. – Санкт-Петербург: Первая образцовая типография, 2015. – 996 с.

15. Маршрутизатор Cisco 2901 K9 [Электронный ресурс] : Сетевые решения. 2014. – Режим доступа: https://nnetwork.ru/marschrutizatory/2900-seriya/cisco2901-k9.html

16. Маршрутизатор Cisco 2901 K9 [Электронный ресурс] : Сетевые решения. 2014. – Режим доступа: https://nnetwork.ru/marschrutizatory/2900-seriya/cisco2901-k9.html

17. Винокуров, В. М. Маршрутизация в беспроводных мобильных Ad hoc-сетях. Доклады ТУСУРа, № 2 (22), часть 1. / В. М. Винокуров, А. В. Пу-

говкин, А. А. Пшенников, Д. Н. Ушарова, А. С. Филатов. – 2010. – 5 с.

18. Правила оформления списка литературы и библиографических ссылок [Электронный ресурс] : Чебоксарский институт (филиал). 2016. – Режим доступа: http://www.polytech21.ru/rekomendatsii-po-oformleniyu

19. Преобразование dBm в милливаты [Электронный ресурс] : Интернет магазин телекоммуникационного оборудования. 2018. – Режим доступа: http://zscom.ru/preobrazovanie-dbm-v-millivatty

20. Радиус действия домашнего Wi-Fi роутера [Электронный ресурс] : Проводник инновационных решений для бизнеса и дома. – Режим доступа: http://wifi.kz/articles/radius-wi-fi-routera/

21. Режим WDS – что это такое и как настроить [Электронный ресурс] : Настройка домашнего оборудования. 2017. – Режим доступа: http://nastroyvse.ru/net/vayfay/rezhim-wds-i-ego-nastrojka.html

22. СТО 4.2–07–2014 Стандарт организации. Система менеджмента качества. Общие требования к построению, изложению и оформлению документов учебной деятельности. Взамен СТО 4.2–07–2012; дата введ. 30.12.2013. – Красноярск, 2014. – 60 с.

23. Что такое структурная схема [Электронный ресурс] : Школа для электрика. 2008-2018. – Режим доступа: http://electricalschool.info/main/electroshemy/848-chto-takoe-strukturnaja-skhema.html

24. Что такое функциональная схема [Электронный ресурс] : Школа для электрика. 2008-2018. – Режим доступа: http://electricalschool.info/main/electroshemy/849-chto-takoe-funkcionalnaja-skhema.html

25. Попков, Г. В. Mesh-сети: перспективы развития, возможные применения. / Г. В. Попков, – Новосибирск: СО РАН, 2012. – 6 с.

26. Вишневский, В. Mesh-сети стандарта IEEE 802.11s: протоколы маршрутизации. / В. Вишневский, Д. Лаконцев, А. Сафонов, С. Шпилев. – Первая миля, 2009. – 6 с.

27. Wi-Fi: неочевидные нюансы (на примере домашнего Wi-Fi) [часть 1] [Электронный ресурс] : Крупнейший в Европе ресурс для IT-специалистов. 2006-2018. – Режим доступа: https://habr.com/post/ 149418/

28. Cisco Wireless LAN Controller (WLC) Configuration Best Practices. Release 8.1. / Cisco Systems, Inc. – 64 с.

29. OMNet++ Simulation Manual. Version 5.2. / Andras Varga and OpenSim Ltd. 2016. – 529 с.

30. OMNet++ User Guide. Version 5.2. / Andras Varga and OpenSim Ltd. 2016. – 166 с.

31. Technical Note. Removal of TKIP from Wi-Fi Devices. / Wi-Fi Alliance, 2015. – 3 с.

32. Wireless Access Point Features. IEEE 802.11a/b/g. / SPA Computers (P) Ltd. 2010. – 10 с.

ПРИЛОЖЕНИЕ А

Листинг программы модели беспроводной сети

DStand.ini:

```
[Config UDP]
description = UDP_Settings
network = DStand
sim-time-limit = 65s

*.*P*.networkLayer.arpType = "GlobalARP"

*.CP*.numUdpApps = 1
*.CP*.udpApp[0].typename = "UDPBasicApp"
*.CP*.udpApp[0].destAddresses = "AP0"
*.CP*.udpApp[0].destPort = 5000
*.CP*.udpApp[0].messageLength = 1000B
*.CP*.udpApp[0].sendInterval = exponential(12ms)
*.CP*.udpApp[0].packetName = "Pck_CP"

*.AP0.numUdpApps = 1
*.AP0.udpApp[0].typename = "UDPSink"
*.AP0.udpApp[0].localPort = 5000

*.AP*.wlan[0].typename = "IdealWirelessNic"
*.AP*.wlan[0].mac.useAck = false
*.AP*.wlan[0].mac.fullDuplex = true
*.AP*.wlan[0].mac.maxQueueSize = 5
*.AP*.wlan[0].radio.transmitter.communicationRange = 200m
```

```
*.AP*.wlan[0].radio.receiver.ignoreInterference = true

*.CP*.wlan[0].typename = "IdealWirelessNic"
*.CP*.wlan[0].mac.useAck = false
*.CP*.wlan[0].mac.fullDuplex = true
*.CP*.wlan[0].radio.transmitter.communicationRange = 150m
*.CP*.wlan[0].radio.receiver.ignoreInterference = true

*.AP*.**.bitrate = 100Mbps
*.CP*.**.bitrate = 10Mbps

*.*P*.wlan[0].radio.displayCommunicationRange = true
*.visualizer.physicalLinkVisualizer.displayLinks = true
*.visualizer.physicalLinkVisualizer.packetFilter = "UDPData*"
*.visualizer.networkRouteVisualizer.packetFilter = "UDPData*"
*.visualizer.networkRouteVisualizer.displayRoutes = true
*.visualizer.interfaceTableVisualizer.displayInterfaceTables = true
*.visualizer.dataLinkVisualizer.displayLinks = true
*.visualizer.*LinkVisualizer.lineShift = 0
*.visualizer.networkRouteVisualizer.lineShift = 0

 [Config Static]
description = Static_without_ACK_and_with_Interf
extends = UDP

*.configurator.config = xmldoc("DSconfig.xml")

*.*P*.wlan[0].radio.receiver.ignoreInterference = false
*.*P*.wlan[0].radio.transmitter.interferenceRange = 500m
*.AP2.wlan[0].radio.displayInterferenceRange = true
```

```
*.*P*.forwarding = true
*.configurator.optimizeRoutes = false
*.*P*.routingTable.netmaskRoutes = ""

 [Config Static_ACK]
description = Static_routing_with_ACK_and_CSMA/CD
extends = UDP

*.configurator.config = xmldoc("DSconfig.xml")

*.*P*.forwarding = true
*.configurator.optimizeRoutes = false
*.*P*.routingTable.netmaskRoutes = ""

*.*P*.wlan[0].typename = "WirelessNic"
*.*P*.wlan[0].radioType = "IdealRadio"
*.*P*.wlan[0].macType = "CsmaCaMac"

*.*P*.wlan[0].mac.useAck = true

 [Config AODV]
description = Config_of_AODV_plus_movement
extends = UDP

*.AP2.wlan[0].radio.displayInterferenceRange = false

*.CP1.mobilityType = "LinearMobility"
*.CP1.mobility.speed = 12mps
*.CP1.mobility.angle = 180deg
```

```
*.hostType = "AODVRouter"
*.configurator.addStaticRoutes = false
*.visualizer.dataLinkVisualizer.packetFilter = "AODV*"

 [Config Sinario]
description = Turn_off_one_of_AP
extends = AODV

*.AP*.wlan[0].radio.transmitter.communicationRange = 250m

*.*P*.hasStatus = true
*.scenarioManager.script = xmldoc("DSscript.xml")

 [Config Environment]
description = Add_some_trees_on_the_field
extends = AODV

*.physicalEnvironment.config = xmldoc("DSenvire.xml")

*.radioMedium.obstacleLossType = "IdealObstacleLoss"

*.AP*.mobility.initialZ = 2.5m
*.CP*.mobility.initialZ = 1.5m

[Config AddConfig]
description = Configuration_near_to_real
extends = Environment

*.*P*.wlan[0].radio.displayCommunicationRange = false
```

```
*.mediumType = "APSKScalarRadioMedium"
*.radioMedium.backgroundNoise.power = -76dBm
*.radioMedium.mediumLimitCache.carrierFrequency = 2.4GHz

*.*P*.wlan[0].radioType = "APSKScalarRadio"
*.*P*.wlan[0].radio.carrierFrequency = 2GHz
*.*P*.wlan[0].radio.bandwidth = 20MHz
*.AP*.wlan[0].radio.transmitter.power = 10mW
*.CP*.wlan[0].radio.transmitter.power = 3.5mW
*.*P*.wlan[0].radio.transmitter.preambleDuration = 10us
*.*P*.wlan[0].radio.transmitter.headerBitLength = 0b
*.AP*.wlan[0].radio.receiver.sensitivity = -76dBm
*.CP*.wlan[0].radio.receiver.sensitivity = -76dBm
*.AP*.wlan[0].radio.receiver.energyDetection = -76dBm
*.CP*.wlan[0].radio.receiver.energyDetection = -76dBm
*.*P*.wlan[0].radio.receiver.snirThreshold = 4dB

*.AP*.wlan[0].radio.antennaType = "ConstantGainAntenna"
*.AP*.wlan[0].radio.antenna.gain = 3dB

[Config AODV_Ping]
description = AODV_Ping
network = DStandPing
sim-time-limit = 300s

*.configurator.dumpAddresses = true
*.configurator.dumpTopology = true
*.configurator.dumpLinks = true
*.configurator.dumpRoutes = true
```

```
*.configurator.config = xmldoc("DSconfig.xml")

*.*.networkLayer.arpType = "GlobalARP"
*.*.routingTable.netmaskRoutes = ""
*.configurator.addStaticRoutes = false
*.*P*.hasStatus = true

*.CP2.numPingApps = 1
*.CP2.pingApp[*].startTime = 1s
*.CP2.pingApp[*].destAddr = "AP4"
*.CP2.pingApp[*].sendInterval = exponential(50ms)
*.CP2.pingApp[*].printPing = true

*.CP4.numPingApps = 1
*.CP4.pingApp[*].startTime = 1.1s
*.CP4.pingApp[*].destAddr = "AP4"
*.CP4.pingApp[*].sendInterval = exponential(70ms)
*.CP4.pingApp[*].printPing = true
```

DStand.ned:

```
import inet.node.inet.INetworkNode;
import inet.common.scenario.ScenarioManager;
import inet.common.lifecycle.LifecycleController;
import inet.environment.common.PhysicalEnvironment;
import inet.visualizer.contract.IIntegratedVisualizer;
import inet.physicallayer.contract.packetlevel.IRadioMedium;
import inet.visualizer.integrated.IntegratedCanvasVisualizer;
import inet.networklayer.configurator.ipv4.IPv4NetworkConfigurator;
```

```
network DStand
{
    parameters:
        string hostType = default("WirelessHost");
        string mediumType = default("IdealRadioMedium");

        @figure[rcvdPkText](type=indicatorText; pos=380,20; anchor=w; font=,18;
textFormat="packets received: %g"; initialValue=0);
        @statistic[rcvdPk](source=AP0.udpApp[0].rcvdPk; record=figure(count);
targetFigure=rcvdPkText);

        @display("bgi=background/wood50,s;bgb=1200,550");
    submodules:
        AP0: <hostType> like INetworkNode {
            @display("i=device/accesspoint;p=493.63998,148.995");
        }
        AP1: <hostType> like INetworkNode {
            @display("i=device/accesspoint;p=553.83997,266.385");
        }
        AP2: <hostType> like INetworkNode {
            @display("i=device/accesspoint;p=585.445,388.29");
        }
        AP3: <hostType> like INetworkNode {
            @display("i=device/accesspoint;p=726.915,404.845");
        }
        AP4: <hostType> like INetworkNode {
            @display("i=device/accesspoint;p=859.355,443.975");
        }
        CP1: <hostType> like INetworkNode {
```

```
        @display("i=device/cellphone2;p=924.07,519.225");
    }

    visualizer: <default("IntegratedCanvasVisualizer")> like
IIntegratedVisualizer if hasVisualizer() {
        @display("p=70,50");
    }
    radioMedium: <mediumType> like IRadioMedium{
        parameters:
            @display("p=70,130");
    }
    configurator: IPv4NetworkConfigurator {
        parameters:
            @display("p=70,210");
    }
    scenarioManager: ScenarioManager {
        parameters:
            @display("p=70,290");
    }
    lifecycleController: LifecycleController {
        parameters:
            @display("p=70,370");
    }
    physicalEnvironment: PhysicalEnvironment {
        @display("p=70,450");
    }
  connections:
}

Network DStandPing extends DStand
```

```
{
      @display("bgi=background/wood50,s;bgb=1200,550");
   submodules:
      CP2: AODVRouter {
         @display("i=device/cellphone2;p=434.945,114.38");
      }
      CP4: AODVRouter {
         @display("i=device/cellphone2;p=493.63998,221.235");
      }
   connections:
}
```

DSconfig.xml:

```
<config>
        <interface hosts="*P*" address='10.3.15.x' netmask='255.255.255.0'/>
        <autoroute metric='errorRate'/>
</config>
```

DSenvire.xml:

```
<environment>
   <object position="min 625 385 0" orientation="0 0 0" shape="cuboid 10 10 8"
         material="forest" fill-color="200 150 20" opacity="1"/>
   <object position="min 615 400 0" orientation="0 0 0" shape="cuboid 10 10 8"
         material="forest" fill-color="200 150 20" opacity="1"/>
   <object position="min 645 390 0" orientation="0 0 0" shape="cuboid 10 10 8"
         material="forest" fill-color="200 150 20" opacity="1"/>
   <object position="min 655 405 0" orientation="0 0 0" shape="cuboid 10 10 8"
```

```
        material="forest" fill-color="200 150 20" opacity="1"/>
    <object position="min 630 415 0" orientation="0 0 0" shape="cuboid 10 10 8"
        material="forest" fill-color="200 150 20" opacity="1"/>
    <object position="min 670 415 0" orientation="0 0 0" shape="cuboid 10 10 8"
        material="forest" fill-color="200 150 20" opacity="1"/>
    <object position="min 645 425 0" orientation="0 0 0" shape="cuboid 10 10 8"
        material="forest" fill-color="200 150 20" opacity="1"/>
</environment>
```

DSscript.xml:

```
<scenario>
    <at t="8.0">
        <tell module="lifecycleController" target="AP2" opera-
tion="NodeShutdownOperation"/>
    </at>
    <at t="15.0">
        <tell module="lifecycleController" target="AP2" opera-
tion="NodeStartOperation"/>
    </at>
</scenario>
```